1. AMAÇ

Bu politikanın amacı kuruluşun bilgi güvenliği ve kişisel veri gizliliği kapsamındaki tüm olay ve ihlallerin tespit edilmesi, raporlanması, değerlendirilmesi, ele alınması ve sonuçlandırılmasına ilişkin esasları belirlemek; veri sahibine ve ilgili otoritelere yapılacak bildirim süreçlerini tanımlamaktır.

2. KAPSAM

Bu politika

- Bilgi güvenliği olayları ve ihlalleri,
- Kişisel veri ihlalleri ve gizlilik olayları
- Kuruluş bünyesindeki bilgi sistemleri, veri işleme faaliyetleri, kullanıcılar, üçüncü taraflar ve tüm dış hizmet sağlayıcılar,
- Olayın tespiti, sınıflandırılması, değerlendirilmesi, müdahalesi, bildirimleri ve kapanış süreçlerini kapsar

3. SORUMLULUK

Bu politikanın uygulanmasında tüm çalışanlar, Her türlü olay ve ihlali gecikmeksizin bildirmekle yükümlüdür. Üst Yönetim; Gerekli kaynakları sağlar ve süreci gözetir. Önemli/hassas olaylarda karar mercii olarak devreye girer. SOME Ekibi; Olayı teknik açıdan analiz eder, log ve kanıt toplar, kök neden analizi yapar ve etkiyi azaltmak, durdurmak ve tekrarını önlemek için aksiyon planlarını yürütür.

4. UYGULAMA

- Bilginin gizlilik, bütünlük ve erişilebilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.
- Yaşanan Bilgi Güvenliği ve Gizlilik olayları bilgi işlem daire başkanlığı siber olaylara müdahale ekibine bildirilmelidir.
- Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.
- Bilgi Güvenliği ihlali oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.
- Güvenlik olayının oluşması durumunda ola anında raporlanmalıdır. İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

- Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurmalıdır.
- Tüm Çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor etmelidir.
- Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, DDOS atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlalleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınmalıdır.
- Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.
- İç problem analizi, adli incelemeler veya üretici kurumdan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.
- Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.
- Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.
- Kanıt toplama; kuruluş içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;
    - Kanıtın mahkemede kullanıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi, Kanıtın niteliği ve tamlığını gösteren ağırlığı.

4.1. Olayın Tanımı

Aşağıdaki durumlar olay/ihlaldir ve derhal kayıt altına alınmalıdır:

- Yetkisiz erişim,
- Veri bütünlüğünün bozulması,
- Kişisel verilerin yetkisiz paylaşımı veya sızması,
- Zararlı yazılım bulaşmaları,
- DDoS saldırıları,
- Sistem arızaları veya hizmet kayıpları,
- Yanlış alıcıya veri gönderimi,
- KVKK kapsamındaki kişisel veri ihlalleri.

4.2. Olayın Bildirilmesi

- Olayı fark eden personel **anında** SOME/KVYS ekibine bildirim yapar.
- Olaylar için standart bir **Olay – İhlal Bildirim Formu** / **Kişisel Veri İhlal Formu** doldurulur.
- Tedarikçiler ve üçüncü taraflar da aynı yükümlülüğe sahiptir.

4.3. Olayın Değerlendirilmesi

Olay değerlendirilirken şu başlıklar incelenir:

Bilgi Güvenliği Açısından

- Etkilenen varlık ve sistemler,
- Olayın kapsamı,
- Etki ve olasılık seviyesi,
- Hizmet kesintisi durumu.

Kişisel Veri Açısından

- İhlale konu kişisel verilerin türü (özel nitelikli dahil),
- Etkilenen kişi sayısı,
- Verinin yetkisiz kişilere geçip geçmediği,
- Aydınlatma yükümlülüğü etkisi,
- Veri sahibine olası zararlar,
- İhlalin **KVKK Madde 12 ve GDPR tipinde 72 saat bildirimi** gerektirip gerektirmediği.

4.4. Olayın Kontrol Altına Alınması ve Müdahale

- Olay derhal izole edilir (hesap kapatma, ağ kesme, erişim iptali vb.).
- Sistem yedekleri, loglar ve dijital deliller **zincirleme kayıt (chain of custody)** ile toplanır.
- Gerekirse ilgili sistem geçici olarak durdurulur.
- Zararın yayılması engellenir.

4.5. Raporlama ve Bildirim Yükümlülükleri

4.5.1. İç Bildirimler

- SOME ve KVYS birimleri üst yönetime rapor sunar.
- Etki büyükse kriz yönetimi devreye girer.

4.5.2. Dış Bildirimler

Kişisel veri ihlallerinde:

- **KVKK'ya 72 saat içinde bildirim yapılması gerekebilir** (ilgili olay türüne göre).
- Etkilenen veri sahiplerinin **makul süre içerisinde** bilgilendirilmesi sağlanır.
- Sözleşme gereği tedarikçilere/müşterilere bildirim yapılması gerekiyorsa süreç uygulanır.

4.6. Düzeltici ve Önleyici Faaliyetler

- Olayın kök neden analizi yapılır.
- Tekrarını önlemek için teknik, idari ve fiziksel kontroller güncellenir.
- Gerektiğinde politika, prosedür, talimat veya eğitimler revize edilir.
- Gerekli durumlarda disiplin süreçleri başlatılır.

4.7. Kayıtların Saklanması

- Olay kayıtları, loglar ve delil niteliği taşıyan tüm belgeler **KVKK ve kurum politikalarına uygun** süre boyunca saklanır.
- Kanıt bütünlüğü korunur.

4.8. Öğrenme ve İyileştirme

- Her olay sonrası değerlendirme toplantısı yapılır.
- Olaydan edinilen tecrübeler yeni kontrollerin oluşturulmasında kullanılır.
- Yıllık BGYS/KVYS gözden geçirmelerinde analiz edilir.

5. YAPTIRIM

- Bilgi güvenliği ve kişisel veri gizliliği ihlali oluşturan davranışlarda;
  - Personel için kurum içi disiplin süreçleri,
  - Tedarikçiler için sözleşme hükümleri,
  - Gerektiğinde yasal mercilere bildirim,
  - KVKK kapsamında idari yaptırımlar uygulanabilir.